Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. *(Currently amended)* A document security system for restricting access to secured documents, the system comprising:

a policy module configured to store at least one process-driven security policy on a computer readable medium, wherein the policy ~~that~~ includes a plurality of states and transition rules, and wherein each of the states is associated with one or more access restrictions, and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another; and

an access manager module configured to access the process-driven security policy and determine whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy.

2. *(Previously presented)* The document security system as recited in claim 1, wherein the one or more access restrictions for the secured document are automatically changed when the state of the process-driven security policy for the secured document changes.

3. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another.

4. *(Previously presented)* The document security system as recited in claim 3, wherein the events are internal or external events with respect to the document security system.

5. *(Previously presented)* The document security system as recited in claim 4, wherein at least one of the events is an external event from a document management system.

6. *(Previously presented)* The document security system as recited in claim 1, wherein one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes.

7. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy to automatically transition from one state to another, wherein the process-driven security policy includes at least a first state, a second state, and a third state, and wherein a first event causes transition from the first state to the second state, and a second event causes transition from the second state to a third state.

8. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy to automatically transition from one state to another, wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state.

9. *(Previously presented)* The document security system as recited in claim 1, wherein the transition rules are based on events.

10. *(Previously presented)* The document security system as recited in claim 9, wherein the transition rules are written in XML.

11. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state, and wherein the secured document is modified when the process-driven security policy for the secured document transitions from the previous state to the current state.

12. *(Previously presented)* The document security system as recited in claim 11, wherein the secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted key, and the key being encrypted must be decrypted in order to decrypt the encrypted data portion, and wherein when the process-driven security policy for the secured

document transitions from the previous state to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state.

13. *(Previously presented)* The document security system as recited in claim 11, wherein, when permitted, access to the secured document is available at a client machine.

14. *(Previously presented)* A method for transitioning at least one secured document through a security-policy state machine having a plurality of states, the method comprising:

(a) receiving an event;

(b) determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; and

(c) automatically transitioning from the former state to the subsequent state of the security-policy state machine when determining step (b) determines that the event causes the state transition.

15. *(Previously presented)* The method as recited in claim 14, wherein the security-policy state machine implements a process-driven security policy, and wherein each state of the security-policy state machine has different access restrictions.

16. *(Previously presented)* The method as recited in claim 14, wherein each of the states of the security-policy state machine have different access policies.

17. *(Previously presented)* The method as recited in claim 16, wherein the security-policy state machine is provided as part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system.

18. *(Previously presented)* The method as recited in claim 14, wherein the transitioning step (c) comprises modifying the secured document to reflect the subsequent state of the security-policy state machine.

19. *(Previously presented)* The method as recited in claim 14, the transitioning step (c) further comprising:

(c1) retrieving an encrypted file key from the secured document;

(c2) decrypting, when permitted by the former state of the security-policy state machine, the encrypted file key to yield a file key;

(c3) subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and

(c4) storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

20. *(Previously presented)* The method as recited in claim 14, wherein the transitioning step (c) further comprising comprises:

(c1) retrieving an encrypted file key from the secured document;

obtaining a private state key associated with the former state of the security-policy state machine;

(c2) decrypting the encrypted file key using the private file key;

obtaining a public state key associated with the subsequent state of the security-policy state machine;

(c3) subsequently encrypting the file key in accordance with the public state key; and

(c4) storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

21. *(Previously presented)* A method for imposing access restrictions on electronic documents, the method comprising:

a) providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of states, and wherein each of the states has distinct access restrictions;

b) providing a reference to the process-driven security policy to at a client computer, the reference referring to the process-driven security policy resident on the server computer;

c) associating the reference to an electronic document;

d) transitioning the process-driven security policy from one state to a current state; and

e) subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy, the current state being informed to the server computer by sending the reference to the server computer.

22. *(Previously presented)* The method as recited in claim 21, wherein the transitioning step (d) is automatically performed based on events.

23. *(Previously presented)* The method as recited in claim 22, wherein the transitioning step (d) is performed at the server computer.

24. *(Previously presented)* The method as recited in claim 21, wherein the associating step (c) associates the reference to a group of documents.

25. *(Previously presented)* The method as recited in claim 21, wherein the method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy.

26. *(Previously presented)* The method as recited in claim 21, wherein the determining step (e) comprises evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document.

27. *(Currently amended)* A computer readable storage medium having ~~comprising~~ computer program code recorded thereon, ~~which~~ that when executed by a processor ~~computer~~, causes ~~the~~ a processor ~~computer~~ to:

detect an occurrence of an event;

determine whether the event causes a state transition for at least one secured document from a former state to a subsequent state of a security-policy state machine having a plurality of states; and

automatically transition from the former state to the subsequent state of the security-policy state machine upon determining that the event causes the state transition.

28. *(Currently amended)* A computer readable storage medium having ~~comprising~~ computer program code recorded thereon, ~~which~~ that when executed by a processor ~~computer~~, causes ~~the~~ a processor ~~computer~~ to:

provide at least one process-driven security policy at a server machine, wherein the process-driven security policy has a plurality of states associated therewith, and wherein each of the states has distinct access restrictions;

provide a reference to the process-driven security policy at a client machine, wherein the reference refers to the process-driven security policy resident on the server machine;

associate the reference to an electronic document;

transform the process-driven security policy from one state to a current state; and

determine at the server computer whether a requestor is permitted to access the electronic document, wherein the access is based on a current state of the process-driven security policy, and wherein the current state is informed to the server computer by sending the reference to the server computer.